Electronic Version
Stylesheet Version v1.1.1

Claims

[c1] A secure credit card, comprising:
a) a counter;
b) a pseudo-random bit sequence generator; and
c) a clock for driving the counter and for driving the pseudo-random bit sequence generator, wherein said clock is operable for an unpredictable number of cycles.

[c2] The secure credit card of claim 1 wherein the counter is a first linear feedback shift register (LFSR).

[c3] The secure credit card of claim 2 wherein the first LFSR has a different initial state compared to other issued credit cards.

[c4] The secure credit card of claim 2 wherein the first LFSR has a different configuration compared to other issued credit cards.

[c5] The secure credit card of claim 2 wherein the first LFSR is configured to have a sequence length of 2^n-1, where n is a number of stages in the shift register.

[c6] The secure credit card of claim 2 wherein the first LFSR has an initial state and configuration set by electronic

fuses.

[c7] The secure credit card of claim 1 wherein the pseudo-random bit sequence generator is a second linear feedback shift register (LFSR).

[c8] The secure credit card of claim 7 wherein the second LFSR has a different initial state compared to other issued credit cards.

[c9] The secure credit card of claim 7 wherein the second LFSR has a different configuration compared to other issued credit cards.

[c10] The secure credit card of claim 7 wherein the second LFSR is configured to have a sequence length of 2^n-1, where n is a number of stages in the shift register.

[c11] The secure credit card of claim 7 wherein the second LFSR has an initial state and configuration set by electronic fuses.

[c12] The secure credit card of claim 1 wherein the clock drives the counter and the pseudo random bit generator for the same number of cycles.

[c13] The secure credit card of claim 1 wherein the clock drives the counter and the pseudo random bit generator for numbers of cycles having a fixed or predictable

mathematical relationship.

[c14] The secure credit card of claim 1 wherein the unpredictable duration is determined by a human action.

[c15] The secure credit card of claim 1 wherein the clock has a clock speed in the range of about 0.1-100 megahertz.

[c16] The secure credit card of claim 1 wherein the counter and pseudo-random bit sequence generators are virtual entities emulated in an electronic processor.

[c17] The secure credit card of claim 1 further comprising a display for displaying numbers produced by the first counter and the second pseudo random bit generator.

[c18] The secure credit card of claim 1, further comprising a means for activating the card for a desired time duration.

[c19] The secure credit card of claim 1, further comprising a means for activating the card for a desired number of transactions.

[c20] The secure credit card of claim 1, further comprising a means for resetting a secure access code or PIN.

[c21] A secure credit card, comprising:
a) a virtually emulated first linear-feedback shift register (LFSR);

b) a second linear-feedback shift register (LFSR) or a second virtually emulated LFSR; and
c) a clock for driving the first and second linear-feedback shift registers, wherein the clock is operable for an unpredictable number of cycles.

[c22] The secure credit card of claim 21 wherein the first LFSR and second LFSR have different initial states compared to other issued credit cards.

[c23] The secure credit card of claim 21 wherein the first LFSR and second LFSR have different configurations compared to other issued credit cards.

[c24] The secure credit card of claim 21 wherein the first LFSR and second LFSR are configured to have a sequence length of 2^n-1, where n is a number of shift register stages.

[c25] The secure credit card of claim 21 wherein the first LFSR and second LFSR each have an initial state and configuration set by electronic fuses.

[c26] The secure credit card of claim 21 wherein the clock drives the first LFSR and the second LFSR for the same number of cycles.

[c27] The secure credit card of claim 21 wherein the clock

drives the first LFSR and the second LFSR for numbers of cycles having a fixed or predictable mathematical relationship.

[c28] The secure credit card of claim 21 wherein the unpredictable duration is determined by a human action.

[c29] The secure credit card of claim 21 wherein the unpredictable duration is determined by a human action.

[c30] A method for authenticating a secure credit card having a linear feedback shift register (LFSR), comprising the steps of:

a) sending from the credit card to a financial institution a card identification number uniquely associated with LFSR settings;

b) sending from the financial institution to the credit card a request for an output of the LFSR after m clock cycles;

c) operating the LFSR for m clock cycles to produce an LFSR output;

d) sending the LFSR output from the card to the financial institution; and

e) comparing the LFSR output with LFSR settings for the credit card to authenticate the credit card.

[c31] The method of claim 30 further comprising the step of

looking up in a database at the financial institution the settings information associated with the card identification number.

[c32] A method for authenticating a secure credit card having a counter and a pseudo-random bit sequence generator (GEN), comprising the steps of:
a) driving the counter and the GEN for numbers of cycles having a fixed or predictable mathematical relationship;
b) transmitting to a financial institution outputs of the counter and GEN after step (a); and
c) authenticating the credit card by comparing the outputs produced in step (b) with settings of the counter and GEN known to the financial institution.

[c33] The method of claim 32 wherein the counter and GEN are driven for the same number of cycles.

[c34] The method of claim 32 wherein the unpredictable number of cycles is determined by a clock operated for an unpredictable duration.

[c35] The method of claim 34 wherein the unpredictable duration is determined by a human action.